DEPARTMENT OF STATE
FY 2008
PRIVACY IMPACT ASSESSMENT
Integrated Personnel Management System (IPMS)

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy Office
E-mail: pia@state.gov

FY 2008 Privacy Impact Assessment
for
Information Technology Projects

Introduction

Section 208 of the E-Government Act requires agencies to conduct a privacy impact assessment (PIA) for all new and significantly modified information technology (IT) projects. This includes projects that are require funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally, and those undergoing Department IT Security Certification and Accreditation (C&A) process. The PIA is an analysis of how information is handled to:

- Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA helps DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified IT systems that contain personally identifiable information (PII) about members of the public. OMB has oversight of implementation of the Privacy Act of 1974, as amended, for all federal agencies.

It is important to note that OMB closely scrutinizes IT project budget requests on the Exhibit 300 based on the answers given on the PIA. The Exhibit 300 is a part of OMB Circular A-11, *Preparation, Submission and Execution of the Budget*. It is published annually at http://www.whitehouse.gov/omb/circulars/index-budget.html .

In addition to other criteria, major IT projects (requests for over $100,000), especially new initiatives, must score well when OMB evaluates the Exhibit 300 Business Cases. The score obtained on the PIA helps to determine whether funding will be given for the project. IT systems scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests (requests for under $100,000) as well as systems undergoing the C&A process. That being said, it is imperative that the attached PIA be fully **completed, certified, and submitted** via e-mail to pia@state.gov .

The Office of Information Programs and Services in the Bureau of Administration (A/ISS/IPS) is responsible for conducting PIAs on IT systems containing PII as part of its Department-wide implementation of the Privacy Act. IPS reviews and scores all PIAs on Exhibit 300 Business Cases. The score reflects how well your system protects personal information. This score will be integrated with the score for security to obtain an overall score. This combined score is incorporated in the submission of Exhibit 300 to OMB. IPS provides the Exhibit 300 to the Office of Information Assurance for purposes of C&A. For non-major systems, IPS retains PIAs for these systems for future use. A guide and a handbook are being provided along with the PIA questionnaire. If you have addition questions please email us at pia@state.gov.

Department of State
FY 2008 Privacy Impact Assessment

The Privacy Staff (A/ISS/IPS) retains a copy of each completed PIA and copies may be provided to the:

- Bureau/office IT Security Manager, when a C&A is required; and
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission when an Exhibit 300 is required.

Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

A. CONTACT INFORMATION

Who is the Agency Privacy Coordinator who is conducting this assessment? (Name, organization, and contact information).

Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

(1) Does this system collect, maintain or disseminate personally identifiable information (PII) about individual members of the public?**

YES _X__ NO___

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".**

If the above answer is YES, please complete the survey in its entirety. If NO, complete the certification page and submit the PIA to the following e-mail address: pia@state.gov.

1) Does a Privacy Act system of records already exist?

YES _X__ NO___

If yes, please provide the following:

System Name _Integrated Personnel Management System _

Number __State-31__

If no, a Privacy system of records description will need to be created for this data.

2) What is the purpose of the system/application?

The Integrated Personnel Management System (IPMS) serves as the Department's primary technical platform for providing human capital management. This comprehensive system was developed to provide a high level of performance and availability. The IPMS has four core applications: (1) the Global Employee Management System (GEMS); (2) Human Resources Online (HR Online); (3) Knowledge Center (KC); and (4) the Post Personnel System (WebPS). Together, these applications have reduced transaction processing overhead, enhanced enterprise-wide data sharing, and have provided employees and their supervisors with the ability to manage independently their personnel-related information through automated workflow processes. The program's overall technical objectives include the automation of human resources functions; unification of disparate hardware platforms; the elimination of duplicate data entry and storage programs; and updating business applications to maintain compliance with amended regulations and legislation. The following are the four core IPMS applications.

1. **The Global Employee Management System (GEMS)** is an Oracle/PeopleSoft-based human resources management application that is the Department's official transaction processing system for all American direct hire employees. GEMS contains the following types of employee and position data: (1) Personal data which includes names, social security numbers, addresses, sex, citizenship, dates and places of birth, marital status, and the names and birth dates of eligible family members; (2) Career data which includes education levels, college(s) attended, major subjects, skill codes, foreign language training and examination scores, performance evaluations; (3) Job history data which includes both current and previous position titles, pay plans, grades, assignment dates, locations, and pending assignment information; and (4) Organizational data which includes organizational hierarchies, accounting information, awards, disciplinary actions, etc.

2. **The Knowledge Center (KC)** is a consolidated HR data repository and reporting system that stores data from multiple Integrated Personnel Management Systems (IPMS) subsystems including the Global Employment Management System (GEMS) and Web Post Personnel (PS). It also includes non-IPMS information from the Bureau of Diplomatic Security (DS), the Foreign Service Institute (FSI), and the Office of Medical Services (M/MED). The KC utilizes the Business Objects Web Intelligence (WEBI) tool suite that allows users to access corporate reports and create their own ad-hoc queries based on the consolidated data in the system.

3. **The Human Resources Online (HR Online)** application provides the front-end security controls and infrastructure for the Bureau of Human Resources intranet applications. It is a single point of entry for nearly 30 of the Bureau's "best in class" applications. It provides a single user registration, logon, and authentication. After logon, it controls access to applications and application data based on roles assigned to the user. Users can access one or more of the following HR applications:

   - Budget Allocation Tracking System (BATS): used for tracking and controlling HR budgets, commitments, obligations, and expenditures against the various HR appropriations, allotments, organizations, functions, and object codes.
   - Career Tracker (CT): a program that assists Senior Foreign Service (SFS) members in keeping a personal inventory of the Career Development Program (CDP) requirements and electives via HROnline.
   - Domestic Staffing Model (DSM): accurately defines the Department's current resource needs as well as linking the Department's request for human resources through sound workload measurement indicators.
   - Employee Profile (EP): an application that serves two functions: (1) reporting an employee's personal information, assignments, grade and award history, language scores, education and training, and EFMs; and, (2) retroactively updating an employee's Employee Profile report for items that need correction prior to 1999.
   - Evacuation Management System (ESM): used primarily by posts and the Family Liaison Office (FLO) during an evacuation to track the departure of evacuees.
   - eTelework: enables employees to submit an electronic Telework Agreement through an automated workflow and approval process. The use of eTelework eliminates the need to store and maintain paper forms and provides electronic data for more accurate federal reporting. The application can be used by all Department of State employees.
   - Family Member Employment Report (FAMER): provides the Bureau of Human Resources Family Liaison Office (DGHR/FLO) with a tool to collect Eligible Family Member (EFM) employment information from posts around the world. This includes information on positions currently within and outside the mission, the work permit situation, and the employment atmosphere.

- File Folder (FOLDER): provides the Executive Office of the Bureau of Human Resources Records and Information Management Division (HR/EX/RIM) with a database for storing and tracking information on employee folders logged in and out of the office. This system sends electronic messages on folder information to Senior Personnel of the folder borrower's bureau or to an e-mail account specified for each bureau. The system uses Bar Code Readers for logging the folders in and out of the office.
- Foreign Affairs Personnel Management (FAPR): a web based application that houses a directory of DoS employees and their personal data.
- Family Liaison Office Subscription Database (FLOS): a web-based application designed for the (HR/FLO) that allows Department employees to subscribe to FLO periodicals released on a recurring basis.
- Foreign Service Bid (FSBID): provides FS employees with a web-based system to prepare and submit bids for open assignments.
- Human Resources Workflow Automation Tracking System (HR WATS): automates business processes and task requests among the Bureau Centers of Excellence (CoE), HR/CSP & HR/RMA. Major functional areas include the ability for users to initiate a task request; the ability for HR specialists to process and view status of tasks submitted to Bureau CoE, HR/CSP & HR/RMA; the ability to create customized reports in a timeline-based format; and lastly, the ability to attach documents to a task request, either at the time of initiation or at any other step in the business process.
- Recruitment, Examination and Employment Tracking Application (REETA): integrates data storage requirements and functionality of three legacy HR/REE access databases used to track recruitment status for both career and non-career employees.
- Office of Casualty Assistance Tracking System (OCATS): provides the Office of Casualty Assistance (M/DGHR/OCA) with a web-based application for tracking calls related to casualties during a crisis.
- Electronic Official Personnel File (eOPF): provides Department employees with the means to review electronic images of documents (e.g., SF-50s, TSP, Health Benefits, etc.) in their administrative folders.
- Presidential Appointments Tracking System (PATS): provides the Bureau of Human Resources, Presidential Appointments Staff Office with the ability to track and maintain Presidential appointments. These appointments include the Civil Commissions, ambassadorial appointments, and Foreign Service Commissions.
- Permanent Change of Station Travel (PCSTRAVEL): allows HR/CDA to prepare travel orders for FS employees transferring to/from assignments; enables HR/EX/BUD to derive accurate obligations to the Post Assignment Travel (PAT) allotment account based on travel order specifics; and HROs at checkin/checkout assignment locations to issue Employee Arrival and Departure Notifications. PCS Travel Proposed

Itinerary module allows employee to propose an itinerary for PCS. Module uses workflow capabilities in GEMS.

- <u>Resume Builder (RB)</u>: a Web-based application that enables Foreign Service (FS) employees to build a resume and make edits as his/her career progresses and personal circumstances change. The resume has a standardized format with sections for employees to list their skill codes, employment history, promotion history, language abilities, training, education, and references.
- <u>Service Computation Date (SCD)</u>: provides Department employees with a tool for calculating the adjusted service computation date to include an employee's prior service.
- <u>Student Loan Repayment Program (SLRP)</u>: one of several recruitment and retention incentives offered by the Department of State. The web based version of the application provides Department employees located domestically and overseas a means to electronically submit requests to be considered for the Student Loan Repayment Program.
- <u>Transfer & Evacuation Management System (TEMS):</u> enables Foreign Service employees to enter their actual transfer/departure/evacuation dates on-line and store some locator information for employees in-transit.

4. **Web Post Personnel (PS)** is the automated standard Human Resources System for managing overseas position and staffing information of Locally Employed Staff (LES), as well as for record keeping and tracking of American employees while assigned abroad for both State and other United States Government (USG) agencies under Chief of Mission authority. The official record of American Government employees is maintained by the respective headquarter agency. Each post's Post Personnel data is loaded into the IPMS nightly via a an FTP process.

Additionally, IPMS has three minor components:

(1) **PAYLINE** is a Web based tool used by HR/OE to determine local compensation plans for locally employed staff at U.S. facilities abroad. The tool incorporates both Watson Wyatt and UNDP methodologies. FSN Pay Scaler integrates the United Nations Data Program (UNDP) country survey methodology and data into the application. PAYLINE is developed in ASP with Oracle backend.

(2) **CAJE** is a job evaluation tool designed to replace the current narrative FSN Position Classification Standards, know as the LEPCH, or the Local Employee Position Classification Handbook. These narrative standards were written in 1978 and only a few standards have been revised to reflect changes in technology, job modernization, or changes to organizations. The CAJE application is an ASP front-end with Microsoft SQL Server databases.

(3) **ABC** (Automated Benefits Computation System) is used to determine whether an employee is in the correct retirement code and eligible to retire on a given date. It also looks if an employee under FSPS has a FSRDS component to his

or her annuity or if an employee under FERS has a CSRS component to his or her annuity. It then computes annuity benefits based on the service performed. ABC is a client/server application with a MS SQL backend.

3) What legal authority authorizes the purchase or development of this system/application?

22 U.S.C. 2581 (General Authority of the Secretary of State)

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

All Department of State Civil and Foreign Service direct hire employees, employee dependents, FS Consular Agents, FS Nationals, Locally Employed Staff (LES), applicants for CS and FS employment, and students. U.S. Citizen direct hires, Foreign National direct hires, dependents, other foreign nationals and resident U.S. citizens employed by U.S. missions abroad.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

The Global Employee Management System (GEMS) is the source for most U.S. Citizen direct hire employee data used by applications under the Integrated Personnel Management System (IPMS). Web Post Personnel is the source for Foreign Service National (FSN) and Local Employee Staff information.

GEMS data includes initial employee information via resume, SF-171, OF-612, or other equivalent employment forms (locator info, check-in forms, assignment cables, etc.). Department-sponsored training data, including language training, is provided by the Foreign Service Institute's Student Training Management System (STMS). Payroll-related information is provided by the Bureau of Resource Management's Consolidated American Payroll and Pension System (CAPPS). Medical data is provided by Office of Medical Services (M/MED), and security clearance information is provided by the Bureau of Diplomatic Security (DS).

The Web PS contains similar information for FSNs and LESs.

HR ONLINE applications, PCSTRAVEL and REETA contain non-employee (e.g., dependents, students, applicants) information:

- PCSTRAVEL - the employee will provide dependent information through submission of the OF-132, *Residence and Dependency Report*;
- REETA – public individuals enrolled/scheduled to take the annual Foreign Service Written Exam (FSWE) will provide Name, SSN,

DOB, Address, etc., to a vendor(s) that administers the exam throughout the country. The vendor(s) will then provide this information to the Office of Recruitment, Examination and Employment (HR/REE) for loading into REETA. In addition, REETA also includes personal information from applicants (including students) for employment. This information is obtained from resumes or other equivalent employment form submitted by the potential hire.

b. What type of information is collected from the source of the information?

The Integrated Personnel Management System (IPMS) collects, stores and processes DoS employee and public information that includes:

- Name;
- SSN;
- Date of Birth;
- Place of Birth;
- Marital Status;
- Mailing Address;
- Emil address;
- Phone Number;
- Race and National Origin;
- Names and birth dates of eligible family members;
- Salary; and
- Education and Training.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

Upon receipt of the Official Personnel Folder (OPF), the Human Resources management specialist manually verifies employee data provided by other Federal agencies. Additionally, data is validated by edit checks, output reports, and quality reviews.

HR relies on the vendor’s contractual obligation to provide accurate data for FSWE enrollments. This data is then cross-referenced against status reports and other counts provided by the vendor during the enrollment period.

For post personnel data, post HR officers manually validate employee records (e.g., SF-171, OF-612, etc.) at time of hiring. Data is made available through reports to data source for review and validation.

b. How will data be checked for completeness?

Employee data integrity and completeness are checked through the use of edits, permitted values, internal management reports and quality reviews

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Yes. All IPMS transactional components (e.g., GEMS, HR Online) contain current data. Information contained in IPMS reporting components (e.g., KC, PRAS) are updated periodically (e.g., nightly, monthly, or as needed).

HR authorized users are responsible for keeping employee data current. Salary and compensation data is updated automatically when compensation plans are updated. In addition, the "Combined Staffing Pattern Report" is reviewed by post HR officers regularly for completeness.

D. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

Yes. IPMS has the ability to derive data and the information is stored electronically in accordance with the IPMS Backup and Recovery Plan.

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

No.

4) Will the new data be placed in the individual's record?

Yes. The derived information may appear on the individual's electronic record or on paper.

5) How will the new data be verified for relevance and accuracy?

Derived information will be verified through internal application edits, data quality checks, employee quality reviews, and management reports.

6) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

IPMS incorporates technical (e.g., Secure Socket Layer (SSL) technology), access control (e.g., user ID and password identification and authentication), and IMPS policy (e.g., least privilege) controls/safeguards that provide adequate protection, non repudiation, integrity, and verification of the data being consolidated.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
Personnel action (SF-50, JF62, and JF62A) reports are used to report changes in personal information to the payroll system. One copy is sent to payroll, one copy is placed in the employee's personnel file, and one copy is given to the employee. Only the HR representatives at the duty station, the employee, and authorized payroll staff have access to these reports. PERTEL cables are sent to the Financial Service Centers (FSCs) for employee identification in the DoS payroll system.

Reports are created on "a need to know" basis for statistical purposes, skills inventories, data quality reviews, internal management controls, and for official reporting both inside and outside of the Department. Access to the reports is limited to authorized users as identified by the system owner.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The data for most IPMS components is stored and maintained centrally. However, data in the Post Personnel consolidated database gets updated nightly from the source systems overseas locations. IPMS incorporates a configuration management approach that ensures the consistent update and use of the Post Personnel data.

2) **What are the retention periods of data in this system?**

The data is maintained until it becomes inactive. When it becomes inactive, it will be retired or destroyed in accordance with published disposition schedules of the Department of State and as approved by the National Archives and Records Administration (NARA).

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**
The procedures can be found in 5 FAH-4, Records Management Handbook.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**
N/A. The system only utilizes authorized technology approved by the DoS IT CCB or HR Local CCB.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

Yes. Individuals can be identified and located by selecting specific information such as name, SSN, employee ID, official duty station and organization code to which assigned; employee home address and other personal information can also be accessed on a strictly limited basis.

User access and record updates are monitored on a daily basis.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Yes. State-31 will be revised when system modifications affect employee information protected by the Privacy Act of 1974.

8) Are there forms associated with the system? YES _X_ NO ___
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

A Privacy Act statement is posted on the login screen. A Privacy Act statement is also included on all HR system access request forms including the following: (1) Request for HR Systems Access; (2) Request to Revise Access for Active Operator; and (3) Request for IPMS Access for Contract Staff.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, other)

Authorized DoS employee users, contractors, managers, HR officers or HR specialists at post, and system administrators have access to the data. Developers do not have “write access” to the production environment.

2) What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?

The user and the user’s immediate supervisor determine the level of “need-to-know” access to IPMS. If the user is a contractor, they must obtain the approval of their respective contracting officer technical representative (COTR). There are three forms used to request access to IPMS: (1) Request for Systems Access; (2) Request to Revise Access for Active Operator; and (3) Request for IPMS Access for Contract Staff.

Access for posts is based on written authorization from an HR or admin officer; a system administrator at the duty station assigns permissions to the HR representative. Based on written authorization from the HR/EX Director, the system manager in Washington assigns access to Washington based employees.

HR employs the concept of least privilege for specific duties and enforces the most restrictive set of rights/privileges needed by users in accordance with the IPMS Access Control Policy.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Access is determined based on user roles. In addition, row (organizational) level security controls in IPMS limit users from accessing/viewing data for employees outside of their organization.

Access can be restricted by user category, function (view only, update status, etc.), and/or functional data group (e.g. positions, employee data, personnel actions).

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)

Systems security controls prohibit access by unauthorized users. IPMS incorporates technical (e.g., Secure Socket Layer (SSL) technology), access control (e.g., user ID and password identification and authentication), and IMPS policy (e.g., least privilege) controls/safeguards that provides adequate protection, non-repudiation, integrity, and verification of the data being consolidated.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

Yes, there are contractors that design, develop and maintain the system. Privacy Act clauses are present in the contracts and in the Statements of Work (SOW). All contractor personnel are required to pass a National Agency Check prior to being assigned to work on the contract.

6) Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Yes. Within IPMS, data is shared internally with:

a. Knowledge Center (KC) (HR); and
b. Personnel Reporting and Statistics (PRAS) (HR).

Data is also shared externally with the following Department systems of records:

- (FSI) STATE 14 - Student Training and Management System (STMS);
- (RM) STATE 30 - Consolidated American Payroll and Pension System (CAPPS);
- (MED) STATE 24 - Medical Services (MEMS); and
- (DS) State 36 - Security Clearance.

7) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?

Yes. IPMS data is electronically shared with the Office of Personnel Management (OPM) for Enterprise HR Integration (EHRI) system purposes.

8) Who is responsible for assuring proper use of the SHARED data?

The Director General of the Foreign Service and Director of Personnel.

ADDITIONAL COMMENTS: *(optional)*